UNITED STATES DISTRICT COURT
FOR THE
DISTRICT OF VERMONT

UNITED STATES OF AMERICA v. JAMES COYNE, Defendant. and UNITED STATES OF AMERICA v. HILARY DENAULT-REYOLDS, Defendant.	Case No. 5:16-cr-154-01 Case No. 5:17-cr-21-01

DECISION ON MOTIONS TO SUPPRESS EVIDENCE AND STATEMENTS, MOTION TO STRIKE AND MOTION FOR BILL OF PARTICULARS

The warrantless review of electronically-transmitted images by electronic service providers ("ESPs") in partnership with law enforcement raises significant constitutional issues. In these two cases, defendants charged with possession of child pornography have moved to suppress evidence obtained through searches of their homes. Both defendants argue that the review of their private electronic communications which later formed the basis for search warrant applications violated their rights under the Fourth Amendment. In addition, Defendant Denault-Reynolds contends that he was subjected to interrogation after his arrest in violation of *Miranda v. Arizona*, 384 U.S. 436 (1966) and the due process clause.

The court held two days of evidentiary hearings in both cases on November 30, 2017 and January 16, 2018.[1] The cases are not consolidated since the offense conduct is unrelated and there is no connection between the actions of the defendants. The evidence concerning the review of images and the generation of tips to law enforcement is substantially similar. For this reason, the court permitted the Government to call the witnesses related to the process of electronic review at a common evidentiary hearing. Both defendants were represented by their own counsel and each received a full opportunity to cross-examine the prosecution's witnesses.

Findings of Fact

I. Electronic Review of Images

The transmission of electronic images is commonplace. With the development of email, text messages, peer-to-peer file sharing, electronic bulletin boards and chat rooms, social media, and other forms of communication, there are innumerable opportunities to exchange still and video images. The attachment of images to emails, texts, and social media has become routine for millions of ESP customers.

The flow of images over the Internet has had at least one severely negative consequence. It has revitalized the illicit trade in child pornography. The increase in public access to the internet between the 1980s and 2000 resulted in a dramatic increase in the exchange of child pornography. For the first time, images could be transferred from one viewer to the next easily and with relative anonymity. Internet sites of many kinds enabled people interested in child pornography to contact one another with little apparent risk of detection.

Congress has responded to this serious social ill through multiple statutes criminalizing possession and distribution of child pornography. Since 1988, federal legislation has focused on

[1] The court has GRANTED the motions to consolidate hearings in both cases. Many of the transcripts and documents cited below have been filed in both cases. For convenience, unless indicated otherwise, the court cites to the documents filed in *United States v. Denault-Reynolds*, No. 5:17-cr-21-01.

the role of the Internet in fostering the exchange of child pornography.[2] Criminal penalties were increased through enactment by Congress of strict federal sentencing guidelines for child pornography offenses. The number of prosecutions increased greatly. See United States Sentencing Comm'n, *Federal Pornography Offenses* 3-16 (2012) (describing increases in convictions between 2004 and 2011).

Law enforcement's ability to detect child pornography increased through development of the "PhotoDNA" program in 2010 by Dartmouth College professor Hany Farid and the

---

[2] Prior to the rise of the Internet, Congress passed the Protection of Children Against Sexual Exploitation Act in 1977 and the Child Protection Act in 1984. See Pub. L. No. 95-225, 92 Stat.7 (1978): Pub. L. No. 98-292, 98 Stat. 204 (1984) (codified at 18 U.S.C. §§ 2251-2253.) These provisions banned the use of children under16 – later increased to age 18 -- to produce visual depictions of sexual conduct. Congress added to these protections in 1986 through passage of the Child Sexual Abuse and Pornography Act, which banned advertisements and provided for civil liability. Pub. L. No. 99-628, § 2, 100 Stat. 3510 (1986) (codified at18 U.S.C. §§ 2251, 2255. With enactment of the Child Protection and Obscenity Enforcement Act of 1988, Congress turned its attention to the role of the internet in particular. Pub. L. No. 100-690, § 7512(a), 102 Stat. 4181 (codified at 18 U.S.C. § 2252.) The use of computers to distribute or receive child pornography was specifically outlawed. The Child Protection Restoration and Penalties Enhancement Act of 1990 addressed the issue of possession of child pornography. Pub. L. No. 101-647, § 311, 104 Stat. 4787 (codified at 18 U.S.C. § 2251).

Congressional efforts to outlaw access to obscene materials online in a fashion similar to restrictions on public broadcast have been curtailed by the Supreme Court on First Amendment grounds. The Communications Decency Act, adopted as part of the Telecommunications Act of 1996, addressed access to pornography on the Internet. 47 U.S.C. § 230. It was not limited to child pornography. It was struck down as vague and overly broad in *Reno v. ACLU*, 521 U.S. 844, 874 (1997).

The Child Pornography Prevention Act of 1996 outlawed computer-generated images as well as images of real children. Pub. L. No. 104-208, § 121, 110 Stat. 3009 (codified at 18 U.S.C. § 2256). The prohibition of virtual images was struck down by the Supreme Court in *Ashcroft v. Free Speech Coalition*, 535 U.S. 234, 254 (2002) on overbreath grounds. Congress returned to the issue of virtual child pornography through passage of the Child Online Protection Act, 47 U.S.C. § 231 (1998), which was also struck down by the Court. *Ashcroft v. ACLU*, 542 U.S. 656, 673 (2004). This issue was largely settled through passage of the PROTECT Act in 2008 which prohibits the distribution of material "that reflects the belief, or that is intended to cause another to believe, that the material or purported material is, or contains…[a visual depiction of an actual minor engaging in sexually explicit conduct.]" 18 U.S.C. § 2252A(a)(3)(B). This provision was upheld in *United States v. Williams*, 553 U.S. 285, 307 (2008). The PROTECT Act also imposed new mandatory minimum sentences which were further increased through passage of the Child Protection Act of 2012.

Microsoft Corporation. *See* Hany Farid, *Reining In Online Abuses,* 19 Tech. & Innovation 593, 596 (2018). This program permits an ESP to compare all of the images passing through its servers with a known group of contraband images. For the first time, it became practical to monitor Internet traffic on American ESP networks for images previously identified as child pornography. Microsoft made PhotoDNA available to all ESPs at no cost. It is now widely used to screen most communications passing through an American ESP for child pornography.

II. Role of NCMEC

To understand the implementation of the PhotoDNA program, it is necessary to consider the role of the National Center for Missing and Exploited Children ("NCMEC"). NCMEC functions as a national clearinghouse for information about child abuse. (Shehan Test., Hr'g Tr. 30, Nov. 30, 2017, Doc. 39). NCMEC was established in 1984 by the parents of Adam Walsh who was abducted and murdered in Florida in 1981. (*Id.* at 17.) His parents formed a non-profit corporation to prevent similar tragedies. Since its formation, NCMEC has grown to an organization of 340 employees serving in five general areas. These are the location of missing children, the prevention of child sexual exploitation, training and education, safety and prevention, and child victim and family services. (*Id.*)

NCMEC receives substantial grant money from federal and private sources. (*Id.* at 20.) Sixty-five percent of its current funding is from the federal government. (*Id.* at 22.) ESPs and other technology companies provide substantial in-kind assistance. (*Id.*) NCMEC is governed by a board of directors from a variety of backgrounds, including parents of missing or murdered children. (*Id.* at 24.) Representatives of law enforcement serve on the board in a limited "non-fiduciary" role in which they lack a vote on most decisions concerning the operation of NCMEC.

III. The Cyber Tipline

From its beginnings in 1984, NCMEC has served as a clearinghouse for tips and information from the public and law enforcement about possible child sexual abuse and trafficking, including child pornography. (*Id.* at 19-20.) In 1998, NCMEC formed a Cyber Tipline ("Tipline") to collect and evaluate tips about child sexual exploitation on the Internet. (*Id.* at 31.) In addition, NCMEC added a Child Victim Identification program in 2002 and a "Net Smarts 411" program in 2007. (*Id.* at 29–30.) The Nets Smarts program provides information to members of the public about computer and internet safety. The Cyber Tipline and Child Victim Identification programs are directed at the detection and prevention of child exploitation in individual cases.

Since 1998, the Tipline has received more than 25 million reports. (*Id.* at 31.) Before 2010, the detection and reporting of child pornography images typically required a tip from a human being who had seen potential contraband on a computer or a video player or in a publication. (*Id.* at 35.) The Tipline was not formed by federal legislative mandate. (*Id.* at 32-33.) In 2008, Congress enacted 18 U.S.C. § 2258A. This measure required ESPs to forward information about possible child pornography to the Tipline. In addition, 18 U.S.C. § 2258D allowed NCMEC to view and catalog child pornography as part of its effort to combat the exchange of these images.

In 2010, when PhotoDNA became available, NCMEC held a very large library of contraband images. By 2016, this collection had grown to approximately 80,000 images. Although the law defines child pornography as sexually explicit images of children under 18, the NCMEC collection used in the PhotoDNA program is limited to images of prepubescent children ages 12 and under. Each image is reduced to a unique numerical hash value based on the

statistical measurement of black and white ("grayscale") values at specific quadrants of the photo. Photos passing through an ESP can also be reduced to a unique hash value based on the same grayscale values. The likelihood that a known contraband photo and a transmitted photo share the same hash value is extremely small. Because the hash value is based only on the relative light or dark values of a photo across multiple quadrants, it cannot be used to duplicate the image. It functions instead as a "fingerprint" or highly specific identifier of the photo.

Once the PhotoDNA program detects a match, the ESP begins to generate a "Cybertip" directed to NCMEC. A large and sophisticated ESP such as Microsoft employs its own human reviewers before forwarding the tip. Small ESPs such as Chatstep may choose to forward tips automatically without reviewing any images themselves. In either case, however, the PhotoDNA match starts the process which leads in most cases to a report to NCMEC.

IV. Practices of the ESPs

PhotoDNA is available without charge to any ESP. At the times relevant in these two cases, it was in use by all three ESPs who provided services to the defendants. The three ESPs employed PhotoDNA in different ways.

A. Microsoft-Skype

Microsoft Corporation employs PhotoDNA to review all materials transmitted over its internet programs, including Skype, which is a proprietary communications system offered by Microsoft to its customers. (Lilleskare Test., Hr'g Tr. 7, Jan. 16, 2018, Doc. 42.) In addition to video communications, Skype allows customers to communicate by text message or audio. (*Id.*) Any photograph transmitted as an attachment to a Skype message passes through PhotoDNA and receives a hash value. This value is compared against a collection of contraband hash values developed by Microsoft. These hashes include the original database received from NCMEC as

well as additional hashes of contraband images, which Microsoft employees contribute to the database. *Id.* at 16–17. Microsoft does not receive hash values directly from law enforcement. *Id.* at 18. The hash values it receives may come from other ESPs, from the work of its own employees, or from NCMEC.

If the hash for a transmitted photo matches the hash for a known contraband image in the Microsoft library, the image is sent to a Microsoft employee who reviews it to determine whether it is in fact an image of child pornography. (*Id.* at 19–23.) These employees also review photos that have been identified by customers or others as inappropriate because they contain terrorist content such as beheadings, revenge pornography depicting adults, or other images banned from Microsoft sites. (*Id.* at 21.) These images are not reviewed through PhotoDNA which is limited to searches for child pornography.

Following confirmation by a human examiner that a photo flagged by PhotoDNA is child pornography, the customer's account is shut down and a Cybertip is electronically transmitted to NCMEC. The Cybertip states that a Microsoft employee has reviewed the suspect photo. (*Id.* at 23, 25.)

B. Oath-Yahoo and AOL Messaging Platforms

The second ESP involved in these cases is Oath, which is the successor to Yahoo and America Online (AOL). (Coad Test., Hr'g Tr. 104, Jan. 16, 2018, Doc. 42.) In May and June 2016, Yahoo employed PhotoDNA to review photos transmitted over its platforms. As in the case of Microsoft, Yahoo employees reviewed any hash matches between the PhotoDNA collection of contraband images and the transmitted photos. In the case of PhotoDNA matches, members of an "escalation team" provided a second level of human review. The identification of

a child pornography image by an escalation team member led to the submission of a Cybertip to NCMEC and the closing of the customer's account. (*Id.* at 114–15.)

C. Chatstep

A third ESP involved in these cases is a much smaller company known as Chatstep. Chatstep is a chat platform that permits members to exchange texts and images anonymously. (Gottipati Test., Hr'g Tr. 131, Jan. 16, 2018.) It was founded by two high school friends in 2012 before they entered college. (*Id.*) It includes public rooms, which anyone may enter, and private rooms, which require a password. (*Id.* at 133.) Because Chatstep does not require a member to submit an email address, it appears to be anonymous to the users. (*Id.* at 132.) In fact, every user can be traced through his or her internet protocol (IP) address.

The founders of Chatstep (who were also its only employees) learned that their program was used to exchange child pornography when they began to receive increasing numbers of complaints from other users. (*Id.* at 139.) In 2015, Chatstep received an email from NCMEC advising them that they were required to report child pornography. (*Id.* at 142.) The company installed PhotoDNA and chose to have matches transmitted automatically to NCMEC. In contrast to Microsoft and Oath, Chatstep did not open and review its customers' images.

NCMEC receives a very high volume of Cybertips from ESPs and other sources. By the end of November 2017, it had received 9,000,000 tips in that year alone. (*Id.* at 84.) Over 90 percent concern Internet users outside the United States. (*Id.* at 112.) NCMEC forwards these to foreign police agencies. (*Id.* at 112.) The majority of the domestic tips are reviewed by a human analyst at NCMEC before the tip is forwarded to the designated police agency closest to the person who used the IP address to transmit or receive alleged contraband. (*Id.* at 116.) At the times relevant to these cases, NCMEC employees did not open image attachments unless a staff

member at the ESP had already done so or the material was publicly available. (*Id.* at 56-57.) The purpose of this practice is to preserve the "private search" exception to the Fourth Amendment warrant requirement. (*Id.* at 133.)

V. Facts Specific to Each Defendant

A. Defendant James Coyne

In 2016, James Coyne was the subject of 64 hash matches through his Microsoft Skype account. Microsoft staff reviewed the matches and forwarded them to NCMEC. NCMEC staff reviewed the images and, based upon the apparent location of the Skype customer, sent the tips to Detective Matthew Raymond at the Vermont Internet Crimes Against Children Task Force. Detective Raymond is the contact person in Vermont designated to receive Cybertips on behalf of the State of Vermont. (Raymond Test., Hr'g Tr. 150, Nov. 30, 2017, Doc. 39.)

After receiving and reviewing the Cybertips, including looking at the images themselves, Detective Raymond and Special Agent (SA) Caitlin Moynihan of Homeland Security confirmed that the IP addresses associated with the images were registered to Richard Coyne, Defendant James Coyne's father. (Aff. of Caitlin Moynihan, ¶¶ 14–15, 33–34, Doc. 5.) Through a criminal record check, SA Moynihan learned that James Coyne was convicted for possession of child pornography two years prior and was currently on federal supervised release.

On November 29, 2016, SA Moynihan obtained a warrant to search the residence of James Coyne, and on December 2, 2016, she conducted a search with Det. Raymond and other law enforcement officers. The search resulted in finding a black cellphone containing hundreds of images and videos depicting child pornography that SA Moynihan and Det. Raymond believe belonged to James Coyne. The agents then placed James Coyne under arrest. (*Id.* ¶¶ 44–54.)

James Coyne was charged with possession of child pornography in violation of 18 U.S.C. §§ 2252(a)(4)(B) and 2252(b)(2).

B. Defendant Hilary Denault-Reynolds

NCMEC received two Cybertips from Yahoo and one from Chatstep involving IP addresses registered to Hilary Denault-Reynolds. (Def.'s Ex. O, Aff. of Det. Thomas Chenette ¶¶ 1–6.) These tips went to Detective Raymond who reviewed the attached images, including an image from Chatstep which had not been reviewed by an ESP employee. In reviewing the Chatstep image, Detective Raymond relied upon a Vermont District Court ruling and advice from the Office of the Vermont Attorney General. (*Id.* at 151.) He referred the case to Detective Thomas Chenette of the Burlington Police Department. Detective Chenette obtained a state court warrant to search the Yahoo account associated with the Cybertips. In response to the warrant, Yahoo disclosed multiple text communications sent via Yahoo! Messenger between the account user and others regarding pedophilia and child pornography. (Chenette Test., Hr'g Tr. 190-193, Nov. 30, 2017, Doc. 39.) Det. Chenette obtained a state court search warrant for the home of Mr. Denault-Reynolds, and conducted the search on November 17, 2016 with Det. Raymond, SA Moynihan, and other officers. (Chenette Aff., ¶¶ 10–14.)

Detectives Raymond and Chenette initially conducted a "knock-and-talk," in which they knocked on Mr. Denault-Reynolds's door and asked to speak with him, advising him that he was not under arrest. (Raymond Test., Hr'g Tr. at 153, Nov. 30, 2017, Doc. 39.) They spoke with Mr. Denault-Reynolds in his kitchen for roughly 45 minutes about his Internet service and the online platforms he used. Mr. Denault-Reynolds denied involvement or knowledge of the account associated with the Yahoo Cybertips. During the interview, Det. Raymond advised Mr.

Denault-Reynolds that he was free to consult an attorney or choose not to answer the questions. After concluding the interview, the detectives searched the house. (*Id.* at 157–58.)

During the search, Det. Raymond found a pornographic magazine titled "Barely Legal" and two DVD-R discs hidden in the basement. (*Id.* at 165.) The on-scene forensic examiner reviewed the DVDs and confirmed that they contained child pornography. (*Id.* at 167.) In addition to the DVDs, the forensic examiner also evaluated an HP laptop from the home. His examination revealed that files with names suggesting child pornography had recently been transferred to a USB thumb drive. (*Id.* at 165–69.) Not having found a thumb drive during the search, Det. Raymond began questioning Mr. Denault-Reynolds again. The detective became more confrontational and advised that he would have to "tear the house apart" looking for the thumb drive. (*Id.* at 180–82.)

After receiving no response from Mr. Denault-Reynolds about the location of the thumb drive, Det. Raymond placed him under arrest. He did not administer a *Miranda* warning. As Mr. Denault-Reynolds was being lead out the door in handcuffs, he said that the thumb drive was "in the stairs." After one of the officers on the scene asked "which stairs," Mr. Denault-Reynolds indicated that the thumb drive was located in the basement stairs. The detectives then found the thumb drive and an additional DVD-R disc located behind insulation in the basement stairwell. (*Id.* at 199.) Mr. Denault-Reynolds was transported to the police barracks and administered his *Miranda* warnings. After further review, the forensic examiner confirmed that the discs and thumb drive together contained over 1,500 images and videos of child pornography. (Aff. of Det. Chenette at ¶¶ 17–19.) Mr. Denault-Reynolds was charged with receipt of child pornography in violation of 18 U.S.C. § 2252(a)(2) and possession of child pornography in violation of 18 U.S.C. § 2252(a)(4)(B).

Analysis

I. Motions to Suppress the NCMEC Review

The motions to suppress concerning the NCMEC review raise three questions:

First, is NCMEC a governmental entity or a governmental agent whose actions are subject to the Fourth Amendment?

Second, does the initial review of the defendants' texts and attachments by the electronic service providers insulate the subsequent search by NCMEC under the "private search" doctrine?

Third, does good faith immunity apply to the actions of NCMEC?

A. Reasonable Expectation of Privacy

Consideration of the Fourth Amendment issues begins with the question of whether there is an expectation of privacy in text messages and other electronic communications. The parties agree that the government is not free to review electronic communications without a warrant. See Gov't Post-Hearing Memo. at 12 ("[The prosecution does not mean] to suggest that, as a general matter individuals lack a reasonable expectation of privacy in their entire email accounts." It is undisputed that law enforcement could not engage in the type of warrantless review of content in which Microsoft and Yahoo (now Oath) engaged in these cases. Such a program would be barred by the Fourth Amendment. See *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010).

The court rejects the Government's argument that the user agreements in place between the ESPs and their customers remove any expectation of privacy. The Microsoft agreement notifies the customer that Microsoft may "access, transfer, disclose, and preserve personal data, including your content … when we have a good faith belief that doing so is necessary to (1)

comply with applicable law or respond to valid legal process….". (Coyne Memo. in Opp. to Motion to Suppress, Ex. 2.) The Yahoo (now Oath) agreement notifies the customer that "Yahoo's automated systems analyze all communications content …for... abuse protection." (Denault-Reynolds Memo. in Opp. to Motion to Suppress, Ex. 2.) Chatstep notifies its customers that the company may disclose any information "reasonably necessary to comply with a law… to protect the safety of any person…." (Denault-Reynolds Memo. in Opp., Ex. 3.) These general statements fail to describe the monitoring or the disclosure of content – without legal process such as a warrant or subpoena– to NCMEC and its law enforcement partners. The user agreements cannot serve as wholesale waivers of rights arising under the Fourth Amendment.

B. Status of the three ESPs

It is also clear that the three ESPs involved in these cases – Microsoft, Oath, and Chatstep – are not themselves agents of law enforcement. The court rejects Defendants' contention that the three ESPs involved in these cases were acting as government agents when they monitored the Internet traffic and reviewed the matches provided by PhotoDNA.

The statutory structure alone is sufficient to defeat this claim. Unlike NCMEC, which is identified as the recipient of Cybertip reports, the ESPs receive discretion to monitor their traffic or not. This case provides an illustration. In its initial years, the founders of Chatstep did not install PhotoDNA or in some other way review the content of their customer's text attachments. They violated no law in not doing so. They were subject to mandatory reporting if they learned of child pornography, but without monitoring software in place, they saw and reported nothing. It was only after other customers complained that they decided to take steps to eradicate child pornography from their site. Increasing inquiries from law enforcement agencies also

contributed to their decision. After installing PhotoDNA, they became subject to frequent mandatory report requirements, which they satisfied through an automated link to the Cyber Tipline.

The evidence at the suppression hearing demonstrated that each of the ESPs involved in this case monitor their customer traffic for child pornography for business reasons and not to satisfy any government mandate. The proliferation of child pornography on a site drives away legitimate customers and is contrary to the companies' values. It is for these reasons that the ESPs use PhotoDNA. Unlike NCMEC, they receive no payment from the government concerning Cybertips and have no law enforcement presence at their location to assist with these issues. For Fourth Amendment purposes, they are private actors, not representatives of government.

The remaining issue – and the one on which the hearing focused – is the role of NCMEC in connecting the purely private review by the ESPs with law enforcement through the CyberTip process.

C. Status of NCMEC

The defendants make two claims concerning NCMEC: (1) that it is a governmental *entity* and (2) that it acted in these cases as a governmental *agent*. The court determines that NCMEC is not a governmental entity. In its partnership with law enforcement, however, it serves as a governmental agent. The searches it conducts of the contents of emails and text messages are subject to the exclusionary rule just as if they had been conducted by law enforcement.

1. Entity

The first question is whether NCMEC is a governmental entity. Despite the engaging opinion of then Judge Gorsuch in *United States v. Ackerman*, 831 F.3d 1292 (10th Cir. 2016), the record in this case demonstrates that NCMEC is not a governmental entity. It was formed as a private not-for-profit corporation. It is governed by a board of directors that does not include any governmental representatives among its voting members. For purposes of governance, it continues to operate as a non-profit.

Like many non-profits, NCMEC receives funding both from governmental grants and from private fundraising. NCMEC performs a range of functions related to the protection of children. Some of these are the types of functions that a law enforcement agency might also perform. An example of such a function is the review of suspected child pornography images. Other functions such as the education of teachers and parents about signs of child abuse could be performed by many types of organizations, including but not limited to law enforcement.

As the *Ackerman* case demonstrates, there are many corporations that are governmental entities. The decision focuses on Amtrak, — but it could have identified a host of others. *Lebron v. Nat'l R.R. Passenger Corp.*, 513 U.S. 374 (1995) provides an exhaustive description of corporations formed by Congress and federal agencies commencing with the creation of the first Bank of the United States in 1791. Although they appear in nearly infinite variety, these corporations are almost always created by legislation and the government plays a central role in their governance.

If corporations and independent authorities established by Congress, like Amtrak, are excluded, it is not easy to find examples of privately-formed non-profit corporations that have developed into governmental entities. The *Ackerman* decision proposes only the Tennessee

Valley Authority ("TVA"). 831 F.3d at 1299. Like Amtrak, the TVA was formed through the acquisition of privately-held assets, but the enactment in 1933 of the Tennessee Valley Authority Act, (Pub. L. No. 73-17, 48 Stat. 58 (1933) (codified as amended at 16 U.S.C. §§ 831 et seq.) establishes the public nature of the power utility. The TVA is hardly an example of a private organization that assumed a public nature primarily because it engaged in activities associated with government.

Non-profit organizations do not become governmental entities simply because they are engaged in work of public significance. Non-profits are frequently engaged in activities with broad social importance, including activities in which government also participates. They still retain their private nature. The Supreme Court recognized this principle in *Trustees of Dartmouth College v. Woodward*, 17 U.S. 518 (1819), which is cited in *Ackerman* for the proposition that performing governmental functions may identify a corporation as a public entity. In *Dartmouth College*, however, the Court turned back an effort by the State of New Hampshire to transform the college into a public institution, ruling that Dartmouth was "an eleemosynary and so far as respects its funds, a private corporation." *Id.* at 633–34. The importance of its educational mission as an "object of national concern, and a proper subject of legislation" was specifically *not* a basis for permitting the incorporation of the private college into state government. *Id.* at 634.

It is insufficient to consider only the form and governance of NCMEC. It is also necessary to consider its actions and actual function to determine if it must be considered a governmental entity. *See Horvath v. Westport Library Ass'n*, 362 F.3d 147 (2d Cir. 2004) (recognizing that many factors determine whether a private organization's actions are attributable to the state). In *United States v. Silva*, 554 F.3d 13, 18 (1st Cir. 2009), the First

Circuit identified three factors as "potentially relevant in deciding whether a private party acts as a government [entity]." These are "the extent of the government's role in instigating or participating in the search, its intent and the degree of control it exercises over the search and the private party, and the extent to which the private party aims primarily to help the government or to serve its own interests." *Id.* at 18.

The enactment of federal legislation authorizing the NCMEC Cyber Tipline has been essential to the wholesale review of images through the PhotoDNA process. The government has supported this effort financially and by enacting mandatory reporting requirements applicable to ESPs and permitting NCMEC to maintain a database of contraband images that formed the nucleus for the PhotoDNA collection of banned images. With the legislation in place, NCMEC and federal, state, and local law enforcement cooperate in developing leads that result in individual prosecutions.

NCMEC, however, performs its clearinghouse function without governmental supervision. The evidence in this case is that the tips concerning Mr. Coyne and Mr. Denault-Reynolds were developed through review by the ESPs and further review by NCMEC. The review of the defendants' transmissions occurred without any governmental participation. After the NCMEC review was complete, the information was forwarded to law enforcement. The governmental role is confined to leadership in creating the system of review, providing financial support for the work, and receiving the results. The actual operation of the review system rests in private hands, both at NCMEC and at the ESPs.

From its founding following the death of Adam Walsh, NCMEC has been very clear about its purpose, which has been to protect children from abuse, including sexual abuse. Law

enforcement shares this purpose, but there is no evidence that NCMEC is controlled by federal or state law enforcement agencies.

The ESPs have been very clear about their purpose in identifying child pornography, which is commercial and not primarily altruistic. Obviously the ESPs involved in this case share a moral repugnance for child pornography, but their efforts to detect child pornography and close subscriber accounts involved in its transmission are strongly motivated by business concerns. This court agrees that these factors are important to the analysis, and examines them in turn.

The enactment of federal legislation authorizing the NCMEC Cyber Tipline has been essential to the wholesale review of images through the PhotoDNA process. The government has supported this effort financially and by enacting mandatory reporting requirements applicable to ESPs and permitting NCMEC to maintain a database of contraband images that formed the nucleus for the PhotoDNA collection of banned images. With the legislation in place, NCMEC and federal, state and local law enforcement are able to cooperate in developing leads that result in prosecutions.

NCMEC, however, performs its clearinghouse function without governmental supervision. The evidence in this case is that the tips concerning Mr. Coyne and Mr. Denault-Reynolds were developed through review by the ESPs and further review by NCMEC. The review of the defendants' transmissions occurred without any governmental participation. After the NCMEC review was complete, the information was forwarded to law enforcement. The governmental role is confined to leadership in creating the system of review, providing financial support for the work, and receiving the results. The actual operation of the review system rests in private hands, both at NCMEC and at the ESPs.

In light of these circumstances, the court is not convinced that NCMEC is a governmental entity.

2. "Agent"

Turning to the question of agency, however, the defendants make a much stronger case. NCMEC is performing a traditional police function in collecting crime tips and forwarding these for investigation by local police departments. If NCMEC did not do this work, the FBI or some other agency would have to do it. With the development of the PhotoDNA screening tool, it became possible to identify and investigate thousands of cases of child pornography possession. NCMEC has ably filled that role, but it has done so in the manner of a police agency.

The grounds on which a search by a private entity is subject to the Fourth Amendment "necessarily [turn] on the degree of the Government's participation in the private party's activities, a question that can only be resolved in light of all the circumstances." *Skinner v. Ry. Labor Executives' Ass'n*, 489 U.S. 602, 614 (1989) (internal quotations and citations omitted). *Skinner* concerned the collection of blood alcohol evidence by railroads from their employees. The Fourth Amendment applied because of the strong governmental involvement in the collection and use of this evidence. "The Government has removed all legal barriers to the [alcohol testing] and indeed has made plain not only its strong preference for testing, but also its desire to share the fruits of such intrusions." *Id.* at 615. The Court found that such engagement was a clear indication of the "Government's encouragement, endorsement, and participation, and suffice[d] to implicate the Fourth Amendment." *Id.* at 615–16.

The same level of Government engagement is present in the collection of Cybertips by NCMEC. Section 2258A of Title 18 lays the legal groundwork for the monitoring of Internet traffic and the investigation of child pornography cases. The statute puts in place: (1) mandatory

reporting by ESPs of potential child pornography offenses; (2) identification of the Cyber Tipline operated by NCMEC as the agency authorized to receive reports; (3) mandatory disclosure of Internet address information related to the offense; (4) forwarding of child pornography images and all other available information to NCMEC; (5) discretion by NCMEC to forward reports of offenses to federal, state, and local law enforcement or foreign authorities; (6) a directive to the Attorney General to coordinate reporting activities with foreign governments; (7) fines for failure to report by ESPs; (8) discretion on the part of an ESP to decide whether to monitor traffic from its customers; (9) disclosure to prosecutors and other officials by law enforcement of the results of their investigations; (10) limitations on disclosure to third-parties; (11) authority to NCMEC to disclose offenses to law enforcement and to ESPs; and (12) preservation of reports.

Section 2258C specifically authorizes the hash value technology used in PhotoDNA. Section 2258D grants immunity to NCMEC and its staff for criminal liability arising from the operation of the Cyber Tipline. In short, 18 U.S.C. §§ 2258A–2258E provide the legal authority and protection necessary for the ESPs and NCMEC to screen all images passing through American ESPs such as Microsoft and Google for illegal pornographic content. This level of authorization and engagement is further enhanced by substantial financial support provided to NCMEC by the federal government, as well as the presence within the NCMEC building of representatives of multiple law enforcement agencies.

Other courts have found that these circumstances—which are uncontested in this and other cases—are sufficient to subject NCMEC's activities to Fourth Amendment requirements. *See Ackerman*, 831 F.3d at 1300–04; *United States v. Cameron*, 699 F.3d 621, 644 (1st Cir. 2012); *United States v. Richardson*, 607 F.3d 357 (4th Cir. 2010); *United States v. Miller*, 16-47-

DLB-CJS, 2017 WL 2705963 (E.D. Ky. June 23, 2017); *United States v. Keith*, 980 F. Supp. 2d 33, 41 (D. Mass. 2013).

The consequence of viewing NCMEC as an agent of law enforcement is that its review of electronic communications is subject to the same Fourth Amendment requirements that apply to its partners in law enforcement. For this reason, it is necessary to consider the application of the private search doctrine to NCMEC's review of electronic communications.

D. Effect of the Private Search Doctrine

Because the ESPs are not government agents, their review without a warrant of suspect photos did not violate the Fourth Amendment. Their searches are private searches, conducted pursuant to the terms of service that govern their relationship with their customers. The same cannot be said, however, of the review of images by NCMEC staff acting as government agents serving in lieu of law enforcement. These staff members are also engaged in reviewing suspect photos without warrants. If their activities do not violate the Fourth Amendment, it can only be because the prior ESP review is a private search, which provides an exception to the exclusionary rule.

The Supreme Court has long recognized that the results of a private search are not subject to the exclusionary rule because a search by a private person is not governed by the Fourth Amendment. *United States v. Jacobsen*, 466 U.S. 109, 117 (1984) ("The Fourth Amendment is implicated only if the authorities use information with respect to which the expectation of privacy has not already been frustrated."). So long as the scope of a subsequent search by government agents does not exceed the private search, the results are not suppressed even though the private search may have invaded the subject's privacy rights under state law.

In this case, the NCMEC review of photos following tips from Microsoft and Yahoo did not exceed these companies' private searches. Both companies operate sophisticated review systems that require individual employees to examine each flagged image to confirm that it contains child pornography. These reviews were documented in the materials forwarded to NCMEC. The actions of the NCMEC staff in opening and reviewing the same images duplicated the private search that had already occurred.

Defendants rely upon the *Ackerman* decision as well as the decision of the District of Massachusetts in *United States v. Keith*, 980 F. Supp. 2d 33 (D. Ma. 2013). In both cases, the court determined that no private search had occurred because NCMEC was the *first* organization to open and review the images. AOL was the ESP in each case. At the times relevant, AOL's practice was to forward a Cybertip automatically to NCMEC whenever the PhotoDNA program detected a match.

This court agrees that the private search doctrine does not apply when the photo has not been reviewed by a human examiner at the ESP. But in cases where such a review has occurred, the principles set out in *United States v. Jacobsen,* 466 U.S. 109 (1984) and *Walter v. United States*, 447 U.S. 649 (1980) govern. *Jacobsen* concerned a search of a package by Federal Express employees who notified law enforcement when they found plastic bags of white powder. Agents of the DEA arrived and opened the package for a second time. The first agent to arrive conducted a field test, which detected cocaine. The Court held that although the field test exceeded the scope of the private search, "[a] chemical test that merely discloses whether or not a particular substance is cocaine does not compromise any legitimate interest in privacy." *Id.* at 123. The invasion of a reasonable expectation of privacy occurred when Federal Express opened

the package. Testing the contents did not constitute a second violation for purposes of the exclusionary remedy.

Walter is not to the contrary. After a carton of obscene films were mistakenly delivered to a private company, employees opened the carton and tried, without success, to view the 8-millimeter films. The FBI picked up the films and ran them through a projector. Because law enforcement greatly exceeded the limited examination conducted by the employees, the Court held that the warrant requirement applied. "The projection of the films was a significant expansion of the search that had been conducted by a private party and therefore must be characterized as a separate search." *Id.* at 657.

Walter would result in the exclusion of photos that were not opened by the ESPs. *Ackerman* and *Keith* are decisions consistent with this ruling. *Jacobsen*, however, removes any requirement of complete identity between the scope of a private search and a subsequent search by law enforcement. Looking closely at a photo at NCMEC for signs of a child's location or examining the metadata (coded information embedded in the photo itself) is analogous to field testing a bag of white powder. In both cases, the expectation of privacy was violated when the photo was first reviewed by the government agent. That review was no different than the private search and is therefore excused from the warrant requirement.

Defendants argue that the review at NCMEC was more intense than the review by the ESPs. This is certainly true. After reviewing all photos through the use of PhotoDNA, the human reviewer at Microsoft or Yahoo is concerned only with not acting on a mistake about the content of the photo. Their concern is to determine that a photo contains child pornography before they close the subscriber's account and forward the Cybertip to NCMEC. The safety of the child and the prosecution of the offender are not their direct responsibilities. NCMEC is

directly concerned with these issues and, consequently, their reviewers look more closely at the images, including metadata embedded in the images.

Looking more closely than the private searcher at the same images does not disqualify a government search from the private search exception. See *United States v. Runyan*, 275 F.3d 449, 465 (5th Cir. 2011) ("[T]he police do not exceed the scope of a prior private search [of computer files] when they examine the same materials that were examined by the private searchers, but they examine these materials more thoroughly than did the private parties."). So long as NCMEC is not reviewing images which were not opened by the ESP, the review of the same image by the ESP and NCMEC is subject to the private search exception, even if the NCMEC reviewer looks more closely at the image or looks beneath the visual surface at the accompanying metadata.

The Cybertip from Chatstep received in Mr. Denault-Reynold's case is different because Chatstep had only two employees—its founders—who looked at no photos. The tips Chatstep forwarded indicated that no human review or private search had occurred at the company. The NCMEC software is designed to prevent an individual review of photos that had not already been opened by the ESP, which is what occurred in this case.

Mr. Denault-Reynolds was the subject of three Cybertips. One tip came from Chatstep. It indicated that a NCMEC employee had not opened the image. (Raymond Test., Hr'g Tr. 150, Nov. 30, 2017, Doc. 39.) Detective Raymond is the commander of the Vermont Internet Crimes Against Children Task Force. He opened the image attached to the Chatstep tip because he had reviewed a Vermont state court decision in February 2016 that stated that he could review the images without a warrant. He also relied upon advice from John Treadwell, Chief of the Criminal Division of the Vermont Attorney General's office, to the same effect.

In the absence of a prior private search, some other exigent circumstance, or a search warrant, law enforcement is not authorized to open images sent as attachments to texts and emails. *See* 18 U.S.C. § 2701. As the growing number of cases on this issue illustrates, however, the matter has not been free of uncertainty. An otherwise unconstitutional search undertaken in good faith as a result of uncertainty or a reasonable, if mistaken, belief about the law gives rise to a good faith exception to the exclusionary rule. *See Heien v. North Carolina*, 135 S. Ct. 530, 534 (2014); *United States v. Diaz*, 854 F.3d 197, 204 (2d Cir. 2017). Detective Raymond's action in being the first person in the chain of review to open the image that accompanied the Chatstep tip falls within the good faith exception. For this reason, the court will not exclude evidence or other results of the search despite the Fourth Amendment violation.

After reviewing the three Cybertips, Detective Raymond obtained a search warrant addressed to Yahoo pursuant to 13 V.S.A. § 8102(b)(1). Yahoo produced additional evidence of child pornography. He obtained a second warrant providing for the search of the Coyne residence.

The defense argues that the good faith exception applies only to the execution of an invalid warrant by an officer who relies in good faith on the warrant the court has given him or her. That is a clear example of good faith reliance, but it is not the only one. Searches conducted on the good faith belief that no warrant was necessary are subject to the exception. *United States v. Aguiar*, 737 F.3d 251 (2d Cir. 2013). The exception has also been held to extend to materials collected in violation of the Fourth Amendment in order to obtain support for a subsequent warrant application. *See United States v. Massi*, 761 F.3d 512, 630 (5th Cir. 2014), *cert. denied.*, 135 S. Ct. 2377 (2015) ("The good faith exception to the exclusionary rule applies here where the search warrant, though ultimately obtained as a result of an illegal detention in

violation of the Fourth Amendment, was obtained and executed by a law enforcement officer in good faith and under an objectively reasonable belief that it was valid and relied upon appropriately obtained evidence." Certainly a law enforcement agent who is both the affiant and the executing officer cannot rely in good faith on his own constitutional violations. See *United States v. Falso*, 544 F.3d 110, 133 (2d Cir. 2008) (Jacobs, J. dissenting).

But that is not what occurred here. The record is clear that the detective obtained the subsequent warrants on the basis of a Cybertip process which is employed throughout the nation by NCMEC. There is no evidence that the detective knew that the private search doctrine did not apply to the Chatstep communications because these were never actually searched by Chatstep. The good faith exception applies to his actions in opening the Cybertip and using that information in later search warrant applications.

Mr. Denault-Reynolds's Fifth Amendment Motion

Mr. Denault-Reynolds raises an entirely separate issue concerning the voluntariness of his disclosure of the location of a small thumb drive containing contraband found in the course of the search of his home.

The defense seeks to exclude the thumb drive on the ground that it was discovered as a result of an involuntary statement. The defense does not rely upon the *Miranda* rule because the exclusionary rule does not apply to statements obtained in violation of *Miranda*. It applies only to Fourth Amendment violations. A statement obtained in violation of *Miranda* may be excluded, but evidence discovered as a result of interrogation in violation of *Miranda* is not subject to exclusion. *United States v. Patane*, 542 U.S. 630, 637–38 (2004).

The only statement the Government intends to offer concerning the discovery of the thumb drive is the statement that "it is in the stairwell." Chenette Test. at 213. The defendant

volunteered this statement, which is therefore not subject to *Miranda*. The Government does not intend to offer the second statement ("the basement stairs") because it follows an inquiry from law enforcement while the defendant is in custody and prior to the *Miranda* warning.

The defense argues that evidence obtained as a result of an involuntary interrogation that fails to meet due process standards may be excluded. (Doc. 21 at 23.) The questioning in this case does not qualify as "involuntary." Although Detective Raymond became increasingly confrontational, there is no evidence that he subjected Mr. Denault-Reynolds to physical or mental abuse. After finding the two CDs and the magazine and learning about the thumb drive from the field exam of the computer, Detective Raymond advised Mr. Denault-Reynolds that he would tear the house apart looking for the thumb drive. That was no more than a reasonable forecast of what would happen if Mr. Denault-Reynolds did not tell where the thumb drive was hidden. It was not an improper threat, and law enforcement was within its rights to conduct a destructive search of the house.

Nothing that Detective Raymond said was enough to create an involuntary interrogation. These arise when threats are made against family or violence is threatened or used. *See Harris v. South Carolina,* 338 U.S. 68, 70 (1949); *Brown v. Mississippi,* 297 U.S. 278, 286 (1936). They may also arise when questioning is prolonged or food and other necessities of life are withheld. *See Reck v. Pate*, 367 U.S. 433, 442–43 (1961). The worst that the defense cites is Detective Raymond's testimony that he started his discussion with Mr. Denault-Reynolds in a relaxed, informal manner and became increasingly confrontational as evidence of child pornography was found and it became likely that Mr. Denault-Reynolds had concealed a thumb drive somewhere in the house. These discussions occurred before Mr. Denault-Reynolds was taken into custody. The questions were asked in a non-custodial setting, and they came to an end when he stopped

answering questions and was arrested. The interrogation remained voluntary for purposes of the due process clause.

Conclusion

In *United States v. Coyne*, No. 5:16-cr-154-01, the Motion to Suppress (Doc. 23) is DENIED.

In *United States v. Denault-Reynolds*, No. 5:17-cr-21-01, the Motion to Suppress (Doc. 21) is DENIED, including the aspect seeking suppression of the evidence of the thumb drive.

Remaining Motions

In *United States v. Coyne*, No. 5:16-cr-154-01, the court DENIES as moot the Motion to Strike (Doc. 34). Both parties have now had an opportunity to brief the suppression issues at length, including post-hearing memoranda, and there is no basis for striking the government's memorandum.

In *United States v. Denault-Reynolds*, No. 5:17-cr-21-01, the court DENIES the Motion for Bill of Particulars (Doc. 22). The discovery already supplied by the Government as well as the agreement to provide a limited list of 50 images which will be offered at trial are sufficient to provide adequate notice to the defendant of the details of the charge against him.

Dated at Rutland, in the District of Vermont, this 10th day of April, 2018.

Geoffrey W. Crawford, Chief Judge
United States District Court